¿Tus empleados utilizan Office 365 para trabajar?: 3 tips para que estén protegidos

Con la fuerza laboral global actual, cada vez más organizaciones aprovechan la nube para colaborar y garantizar la continuidad del negocio y la productividad. Microsoft 365, en particular, está ganando terreno como la plataforma de productividad preferida. **¿Cómo pueden las organizaciones y los usuarios estar seguros de que sus sistemas y datos están protegidos en este entorno de nube?**

Si bien Microsoft Office 365 ofrece una serie de capacidades de protección de datos y disponibilidad del sistema, los datos aún pueden dañarse o perderse en función de varias situaciones imprevistas, incluidos cambios y eliminaciones, así como vectores de amenazas maliciosas externas como virus y ransomware.

En este contexto, en Quest Software brindamos tres consejos para reforzar los procesos de seguridad y recuperación de Office 365.

1. **Toma el control con copias de seguridad:** Las aplicaciones SaaS, y la nube en general, son tan susceptibles a interrupciones y desafíos de recuperación como los centros de datos locales tradicionales. Esto incluye fallas de infraestructura o errores accidentales, hasta ataques maliciosos intencionados. Para ayudar a mitigarlos, los equipos de TI deben realizar sus propias copias de seguridad de Office 365. Mantén múltiples copias de de seguridad en diferentes dispositivos y ubicaciones, ya que esta es una de las mejores defensas contra ataques maliciosos. Realizar tu propia copia de seguridad de Office 365 permite a la empresa restaurar datos críticos en otra ubicación o sistema, incluido un recurso local. Esto hace que sea más fácil ayudar a reducir el riesgo de inactividad empresarial, mantiene la productividad bajo control y protege el negocio.

2. **Familiarízate con las políticas de retención de datos:** Office 365 ofrece políticas de retención, pero asegúrate de leer la letra pequeña. No todos se consideran retención de datos a largo plazo requeridos por varias regulaciones de cumplimiento. Además, las políticas de retención no protegen los datos que se modifican de forma accidental o maliciosa. Para reforzarlo, recurre a soluciones de terceros que admitan una estrategia de copia de seguridad 3-2-1, una que le permita a la empresa tener múltiples copias de datos en dispositivos separados y en diferentes ubicaciones. Esto brindará la protección que necesitas y la capacidad de recuperar archivos o datos modificados, dañados o eliminados. Además, no hay límite en cuanto al tiempo que eliges conservar tus datos.

3. **Comprende las conexiones y contextos de los datos de Office 365:** A menudo, no solo son importantes los archivos o correos electrónicos, sino también el contexto y las conexiones que estos correos electrónicos y archivos tienen con otros datos. ¿Imagina intentar reconstruir ese contexto cuando todo lo que tienes son documentos individuales o registros de chat? De aquí es de donde proviene el verdadero valor comercial de Office 365. Considere Microsoft Teams, que se ha convertido rápidamente en una de las aplicaciones de productividad y conectividad más populares

utilizadas por las organizaciones. Teams permite a los compañeros de trabajo compartir y colaborar en documentos y wikis, y comunicarse a través de reuniones de chat y video. Proteger solo los documentos individuales o registros de chat sin el contexto circundante de la estructura del equipo, las conexiones y el historial, significa que el valor comercial de ese contexto está desprotegido.

Conclusión

Es fundamental que las empresas tengan un conocimiento completo de todos los datos en los entornos de Office 365 y lo que hace que estos datos sean importantes para la empresa. Tener esta visibilidad y una sólida comprensión del contexto de todos la información ayudará a garantizar que las organizaciones implementen sólidos procesos de respaldo y recuperación en Office 365.